

# Содержание

**SSH** ..... 3



# SSH

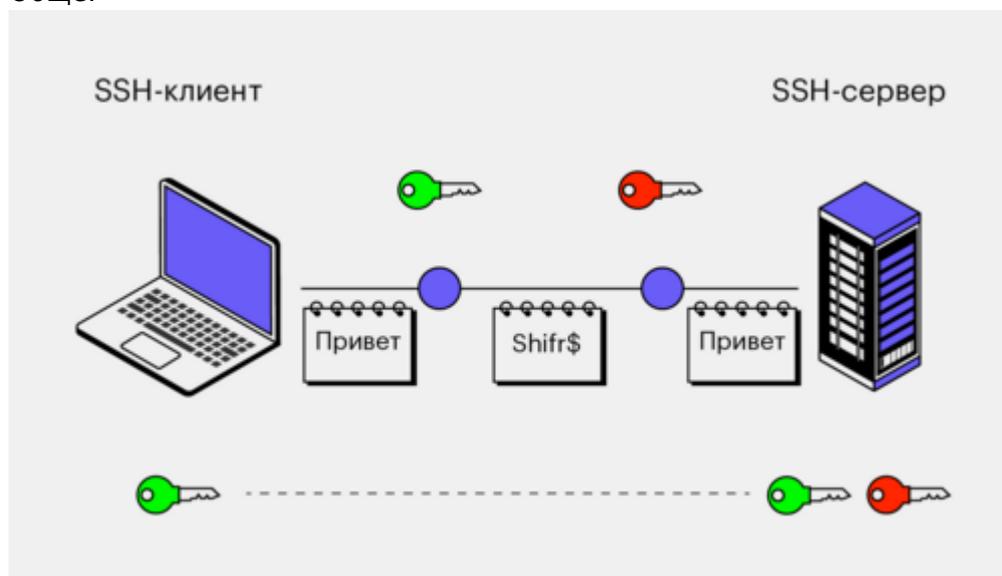
SSH (**Secure Shell**) - протокол сетевого уровня, который используется для безопасного подключения к удаленному серверу, пришедший на замену незащищенному [telnet](#).

В концепции SSH открытый замок представляет публичный ключ, или *public key*. Ключ от замка - приватный ключ, или *private key*.

С помощью публичного ключа мы шифруем данные, а с помощью приватного - расшифровываем. Без приватного ключа даже владелец данных не получит к ним доступа. Приватный ключ важно беречь.

Генерировать ключи можно при помощи [ssh-keygen](#).

Обще:



Подробнее:



1. Клиент отправляет id публичного ключа, заявляя этим, что у него есть соответствующий private key.
2. Сервер шифрует публичным ключом сообщение «вызов» (challenge) и отправляет клиенту. Клиент должен это сообщение расшифровать, зашифровать и отправить на сервер, подтвердив этим наличие у себя private key.

### 3. Установка соединения

Самое соединение защищается при помощи комбинации асимметричного и симметричного шифрования. После успешной аутентификации генерируется симметричный<sup>1)</sup> ключ, называемый *сессионным*. Сессионный ключ может меняться в течении сессии, это называется *key re-exchange*, таким образом подобрать его попросту невозможно, ведь на его подбор уйдет больше времени, чем он будет актуален в рамках сессии.

Помимо шифрования данных, ssh клиент и сервер проверяют<sup>2)</sup> целостность данных, что бы убедиться в том, что они небыли изменены во время передачи.

1)

он симметричный, так как так быстрее шифровать данные

2)

используя HMAC

From:

<https://wiki.radi0.cc/> - radi0wiki

Permanent link:

<https://wiki.radi0.cc/glossary:net:protocols:ssh>

Last update: **2025/11/09 12:07**

